在FMC管理的FTD上配置安全客户端证书身份验证

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 网络图
- 配置
  - 创建/导入用于服务器身份验证的证书
  - 添加受信任/内部CA证书
  - 配置VPN用户的地址池
  - 上传安全客户端映像
  - 创建和上传XML配置文件
- 远程访问VPN配置

验证

故障排除

简介

本文档介绍如何在FMC管理的FTD上使用证书身份验证配置远程访问VPN。

先决条件

要求

Cisco 建议您了解以下主题：

- FMC
- 远程访问VPN的基本身份验证知识
- 手动证书注册和安全套接字层(SSL)基础知识
- 第三方证书颁发机构(CA)，例如Entrust、Geotrust、GoDaddy、Thawte和VeriSign

使用的组件

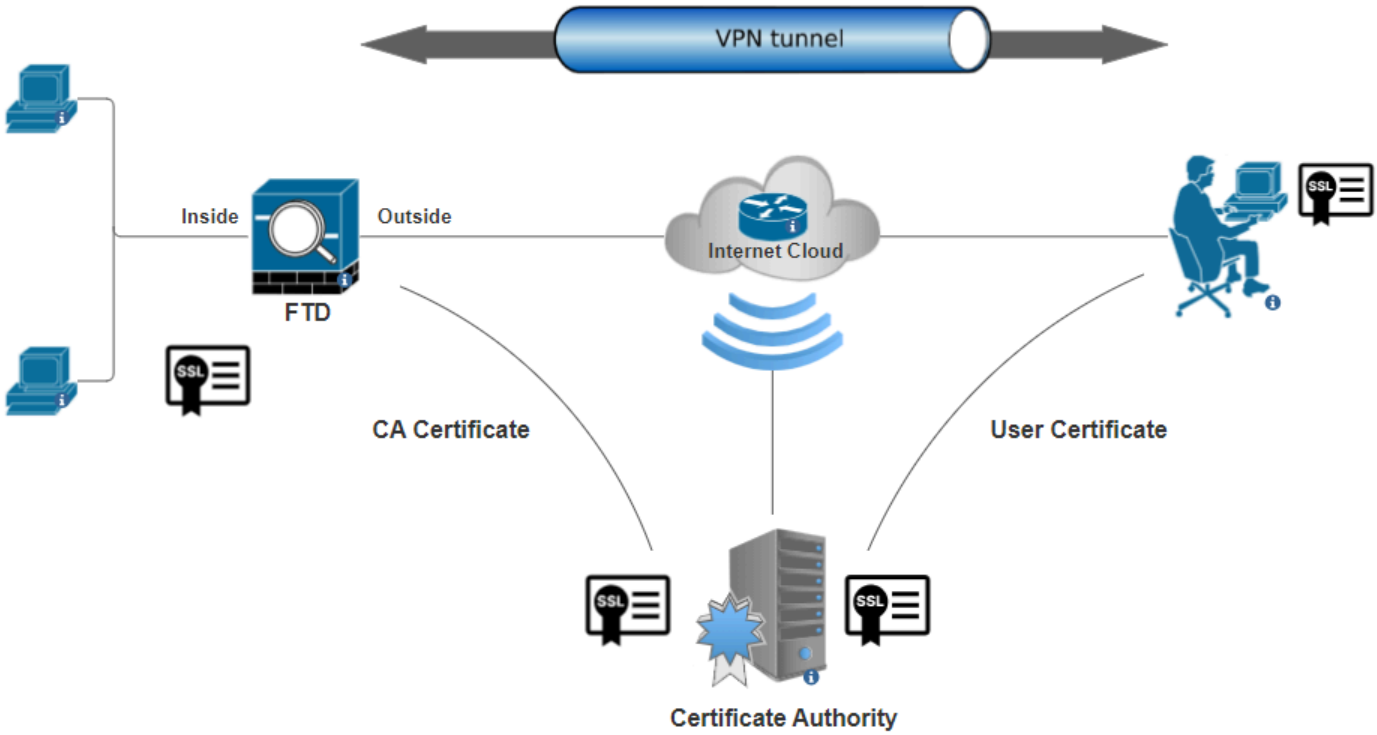
本文档中的信息基于以下软件版本：

- FMC版本7.4.1
- 安全客户端版本5.0.05040
- 安全Firepower威胁防御版本7.4.1
- 作为CA服务器的Microsoft Windows Server 2019

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



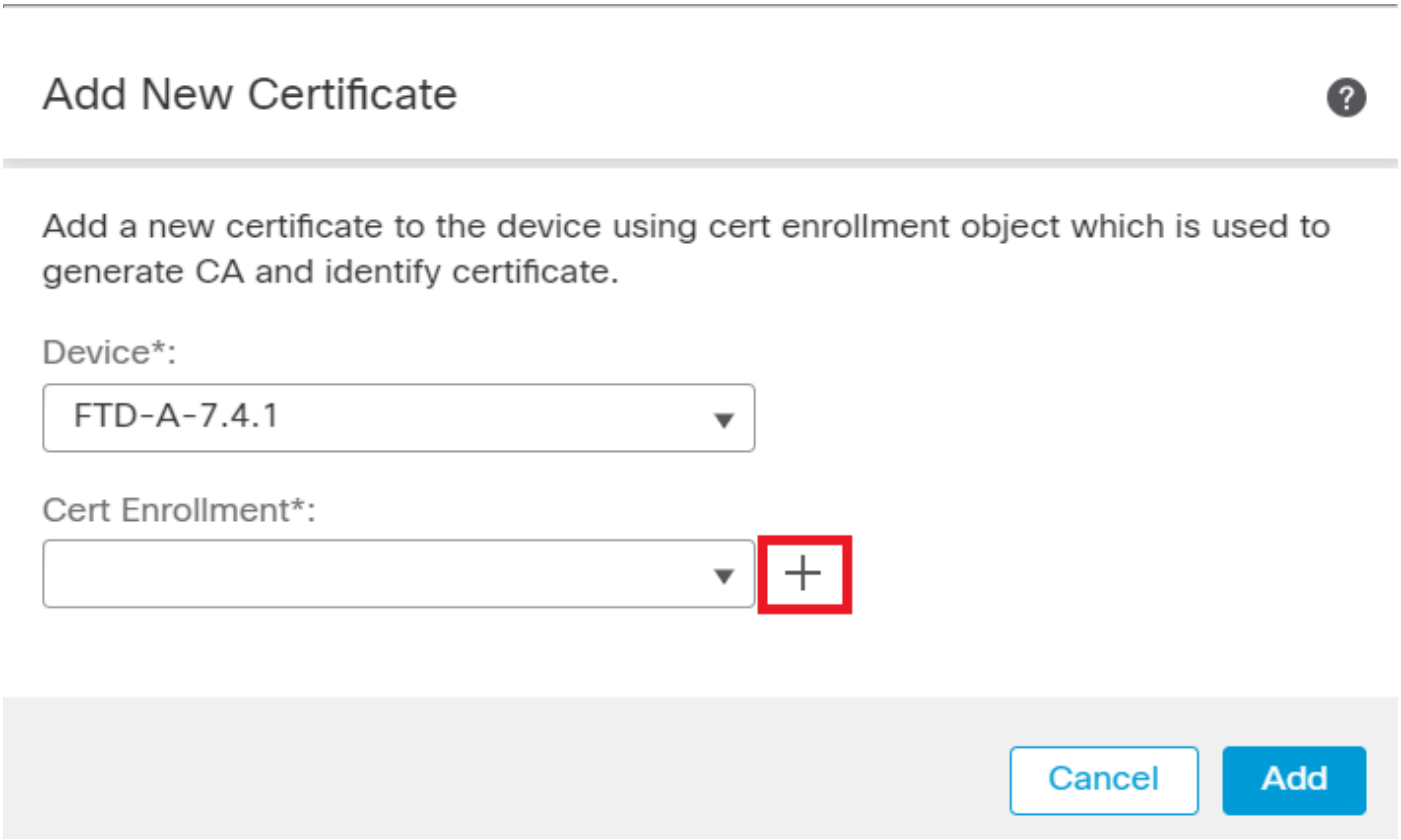
网络图

配置

创建/导入用于服务器身份验证的证书

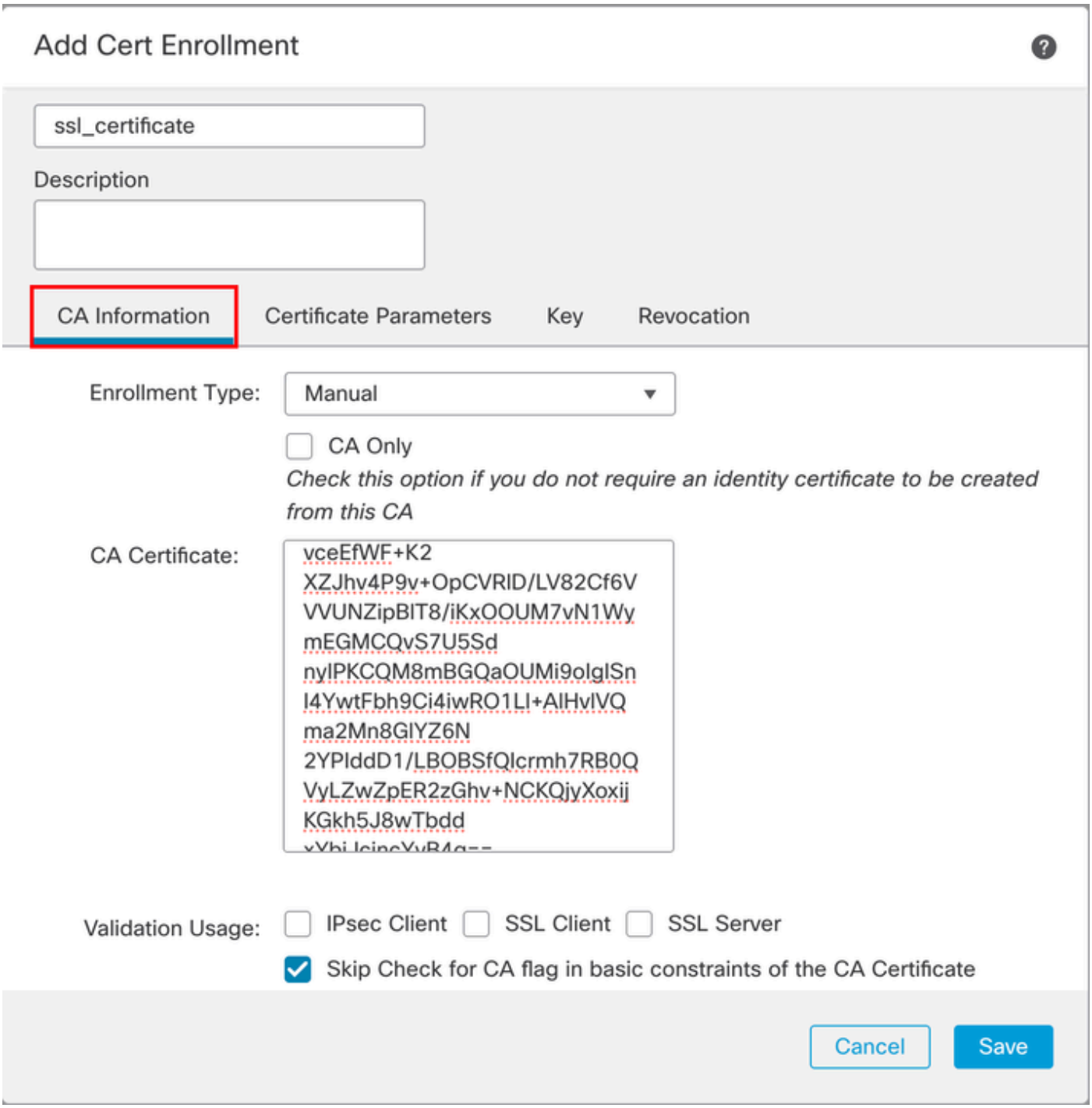
注意：在FMC上，需要证书颁发机构(CA)才能生成CSR。如果从外部源（OpenSSL或第三方）生成CSR，手动方法将失败，并且必须使用PKCS12证书格式。

1.导航到设备>证书，然后单击添加。选择Device，然后单击Cert Enrollment下的加号(+)。



添加证书注册

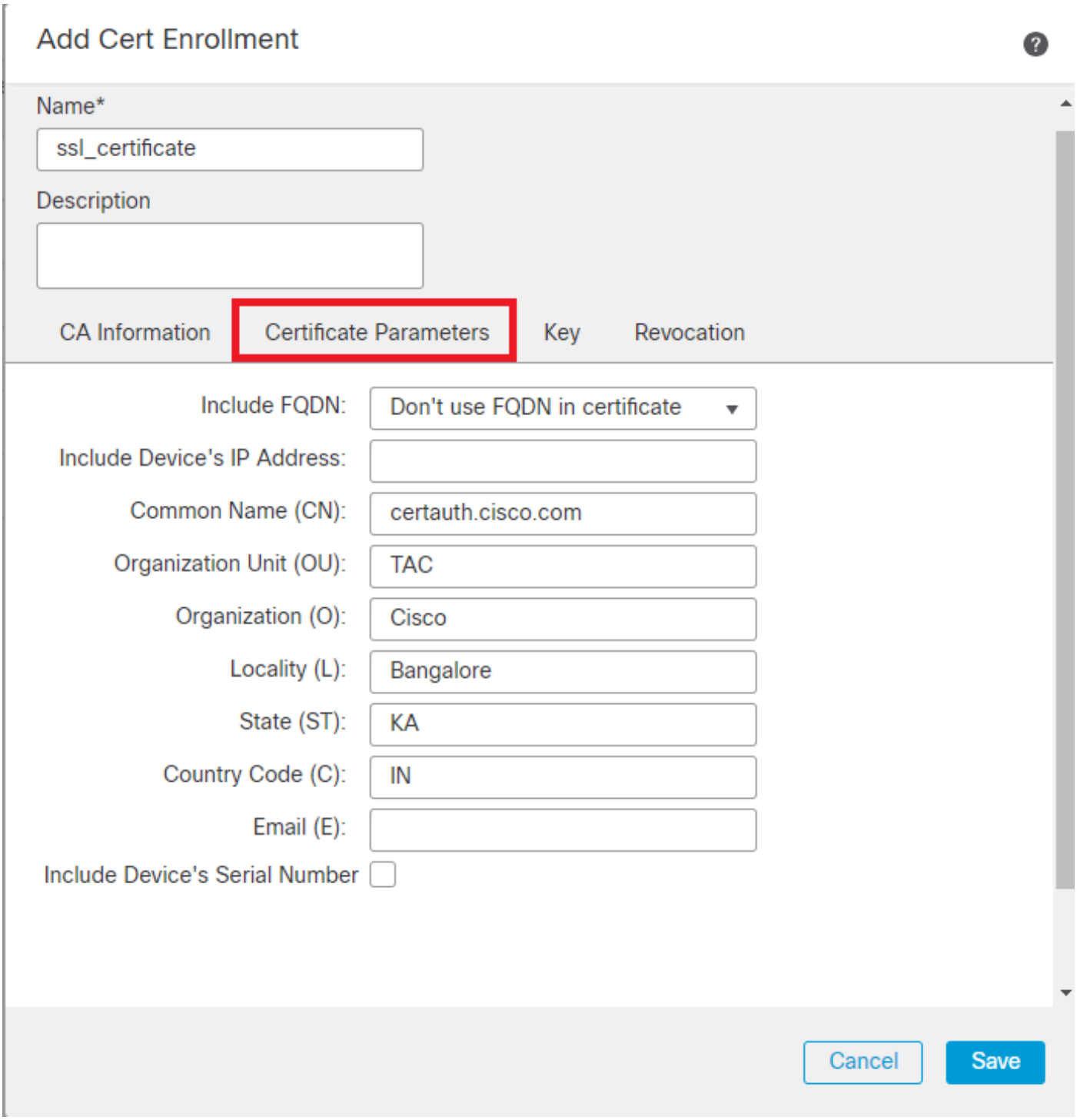
2.在CA Information下，选择Manual作为Enrollment Type并粘贴用于签署CSR的CA证书。



添加CA信息

3.在CA证书的基本约束中选择Skip Check for CA flag as shown in the prior image.

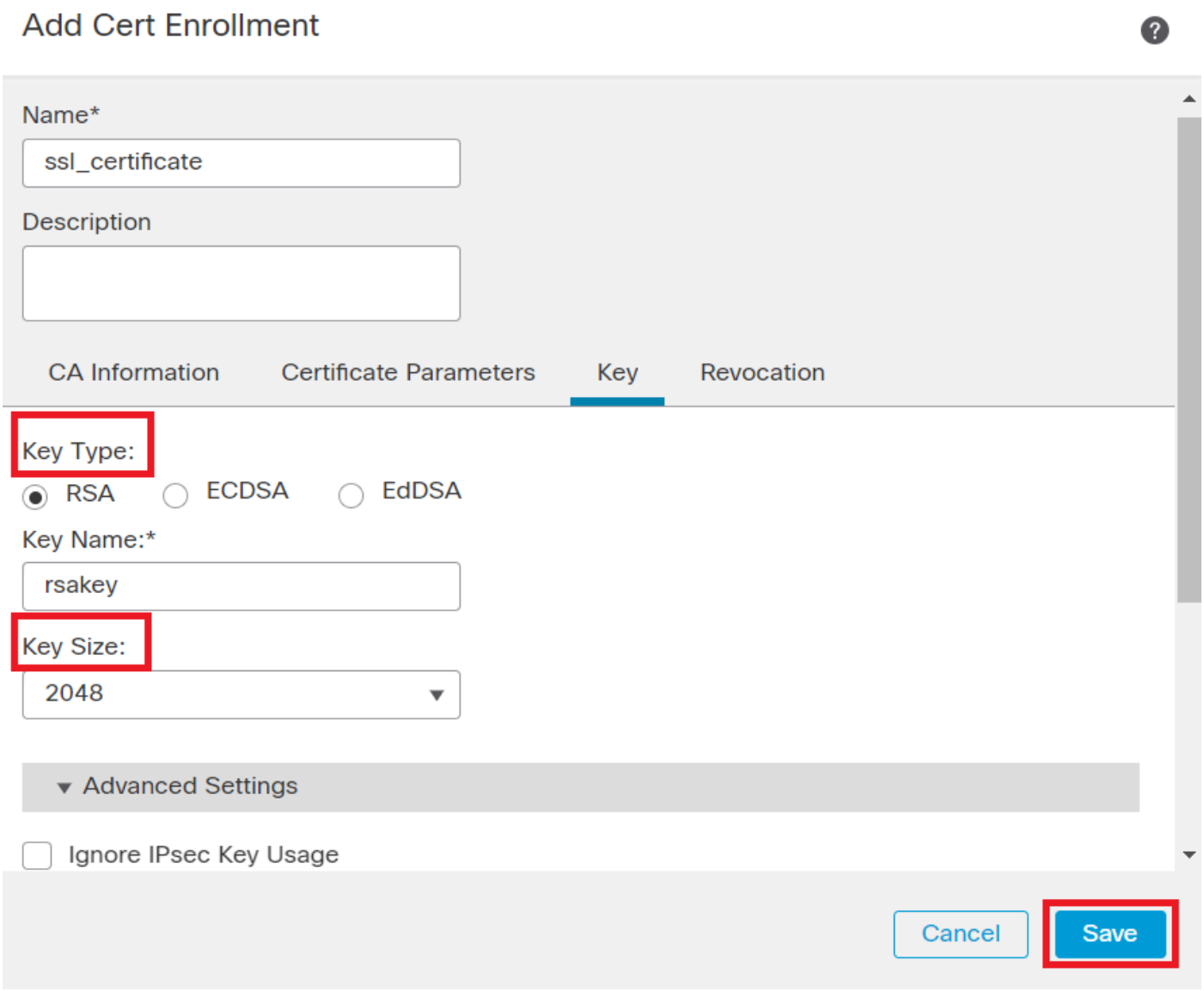
4.在证书参数下，填写主题名称详细信息。



添加证书参数

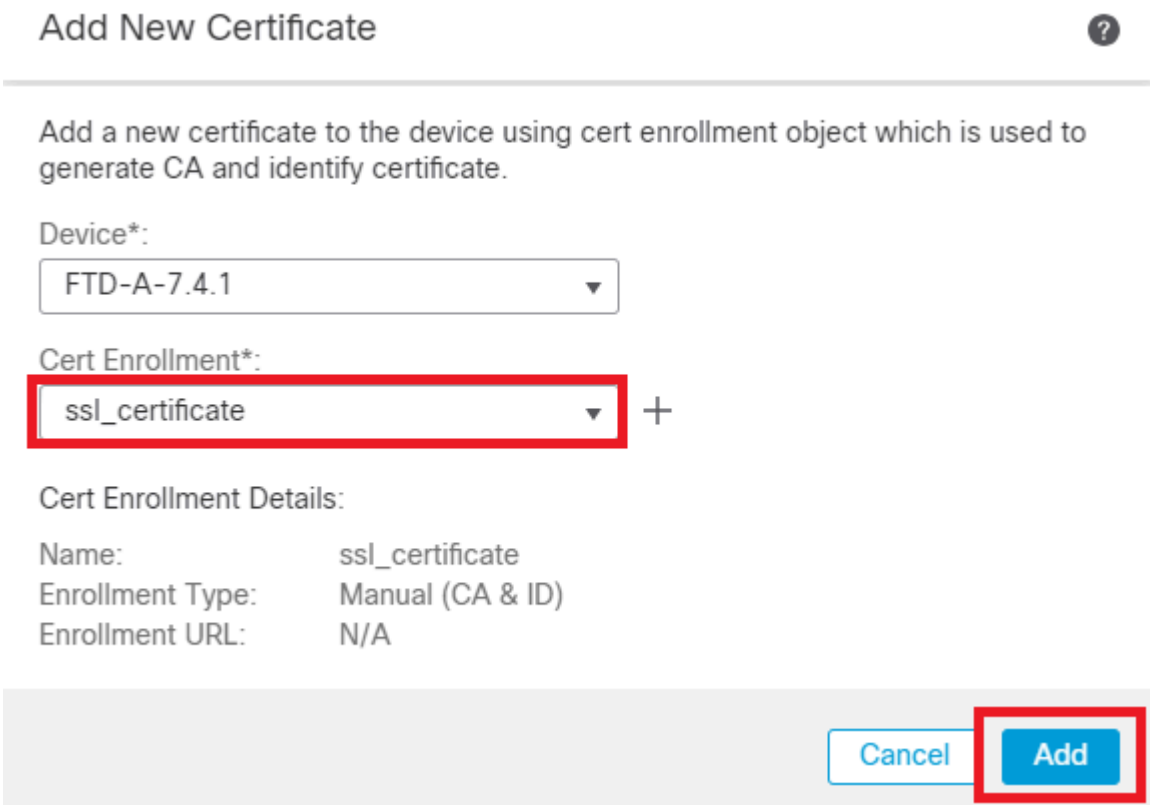
5.在密钥下，选择密钥类型为具有密钥名称和大小的RSA。单击Save。

注意：对于RSA密钥类型，最小密钥大小为2048位。



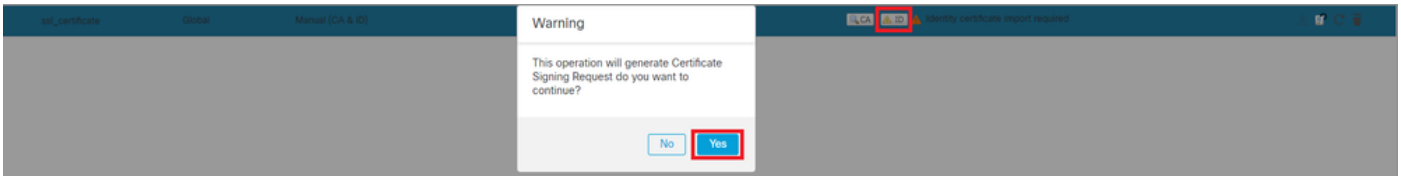
添加RSA密钥

6.在Cert Enrollment下，从刚创建的下拉菜单中选择信任点，然后单击Add。



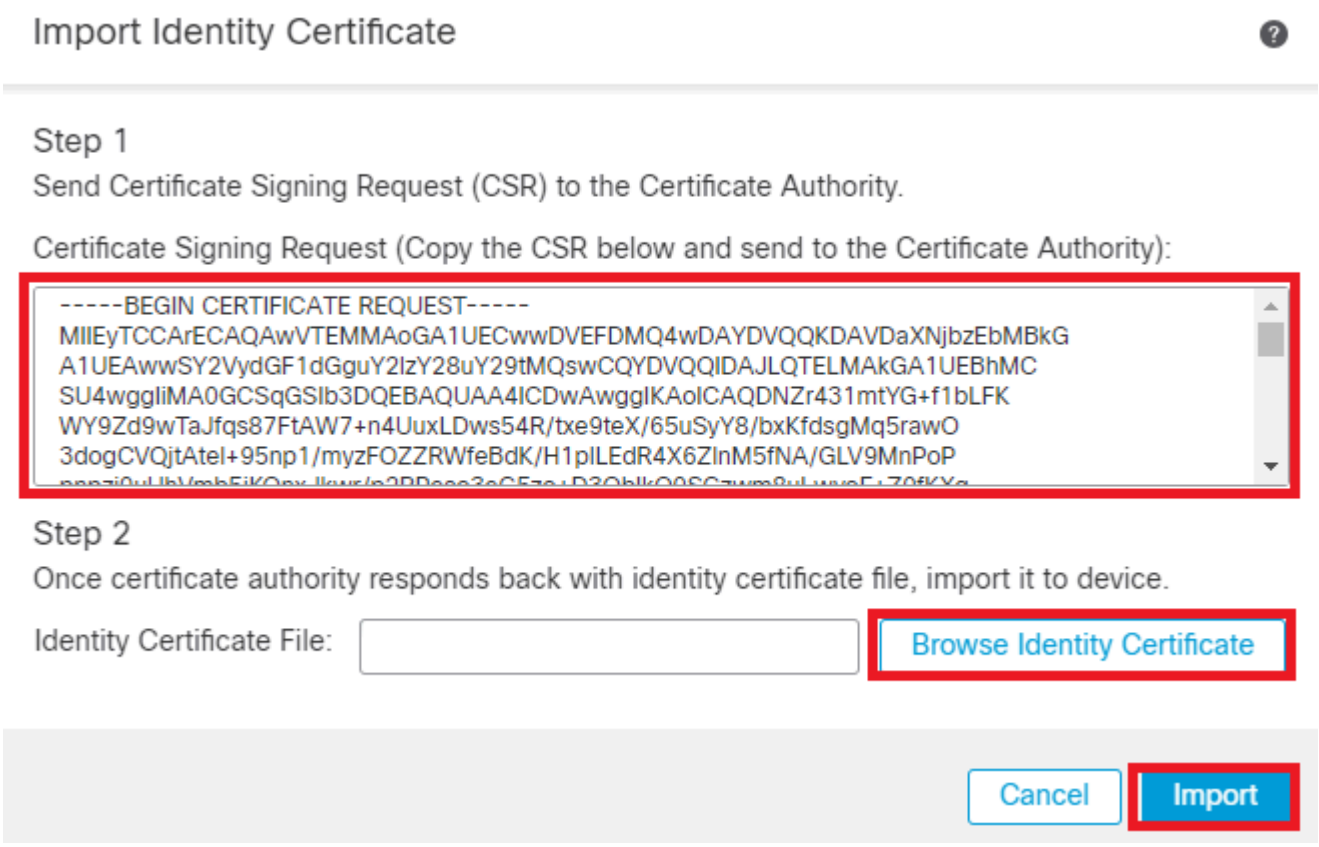
添加新证书

7.单击ID，然后单击是以生成CSR。



生成 CSR

8.复制CSR并确保其由CA签署。CA颁发身份证书后，请点击Browse Identity Certificate并点击Import导入身份证书。



导入ID证书

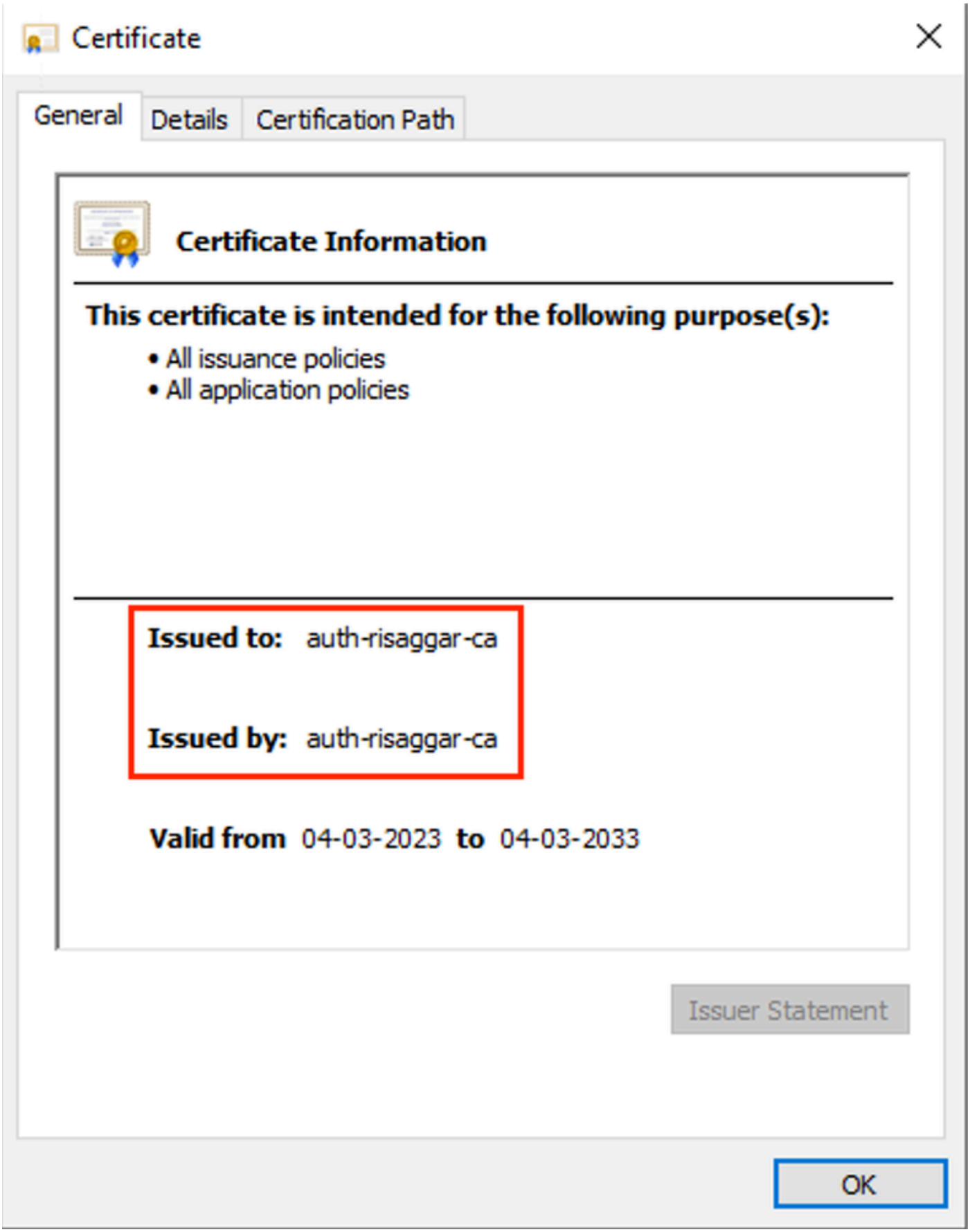
注意：如果ID证书的颁发需要时间，您可以稍后重复步骤7。这会生成相同的CSR，并且您可以导入ID证书。

添加受信任/内部CA证书

1.导航到设备>证书，然后单击添加。

2.选择Device，然后单击Cert Enrollment下的加号(+)。

3.在本示例中，auth-risaggar-ca用于颁发身份/用户证书。

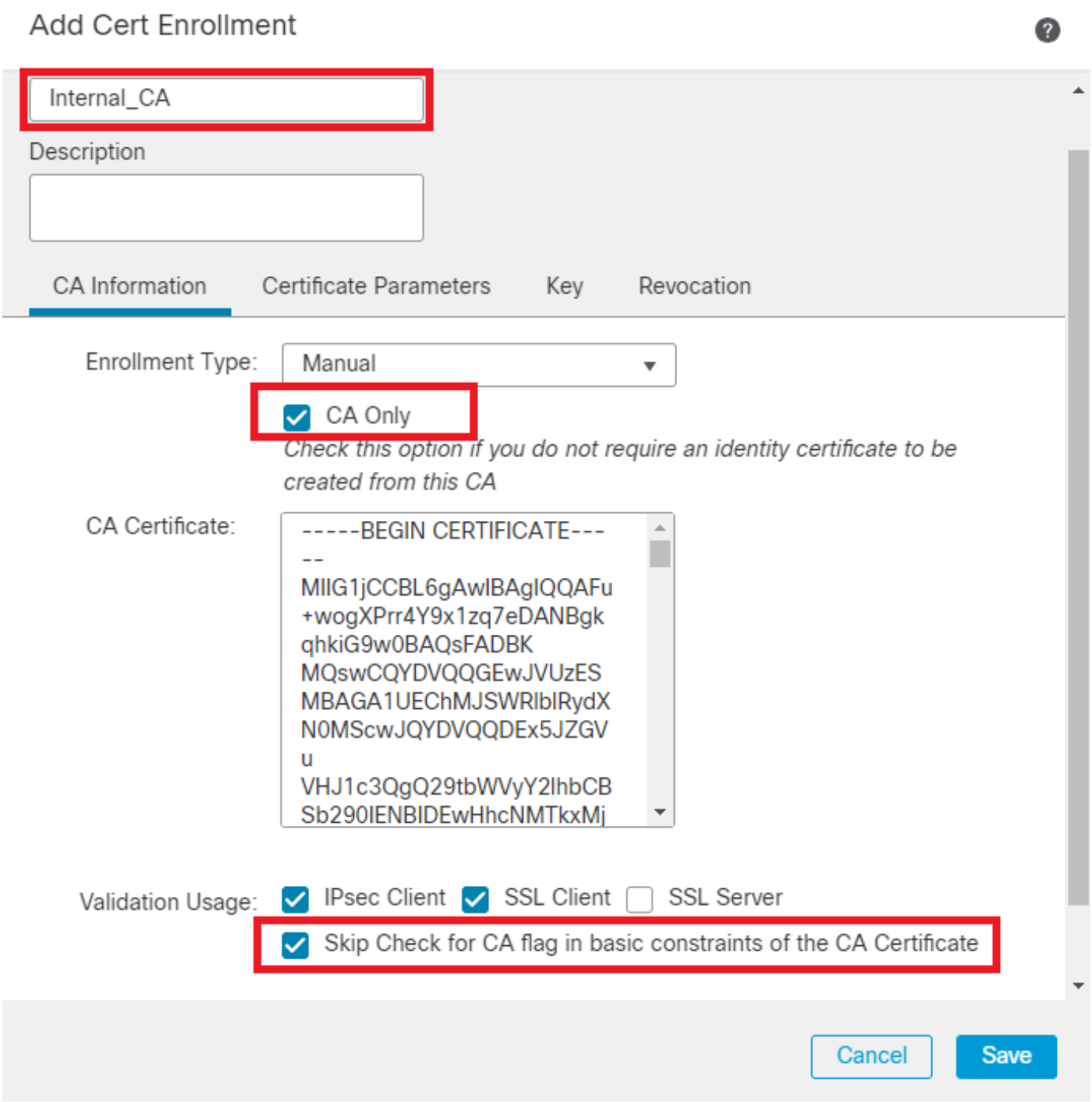


auth-risaggar-ca

4.输入信任点名称，然后选择手动作为CA信息下的注册类型。

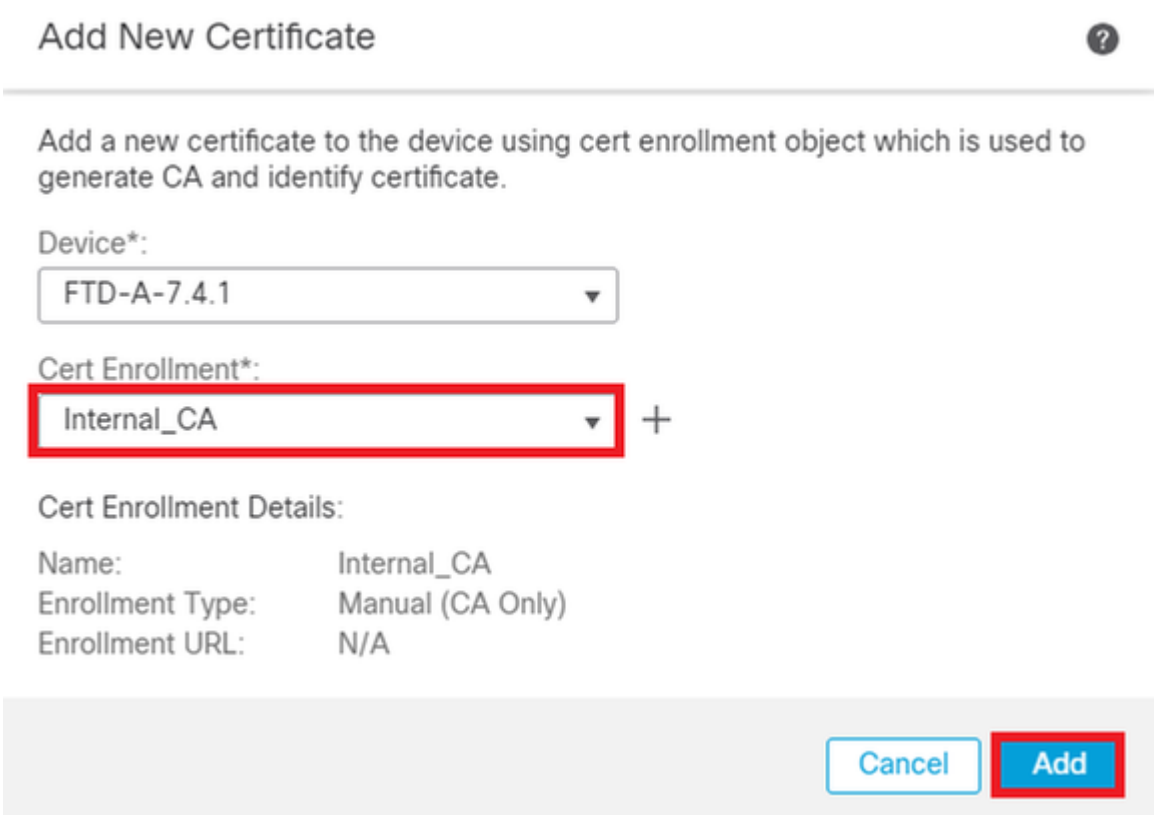
5.选中CA Only并以pem格式粘贴受信任/内部CA证书。

6.选中CA证书基本限制中的Skip Check for CA flag，然后单击Save。



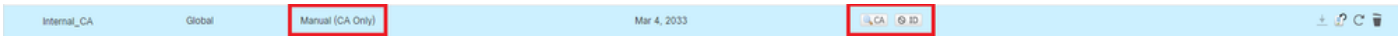
添加信任点

7.在Cert Enrollment下，从刚创建的下拉菜单中选择信任点，然后单击Add。



添加内部CA

8.之前添加的证书显示为：

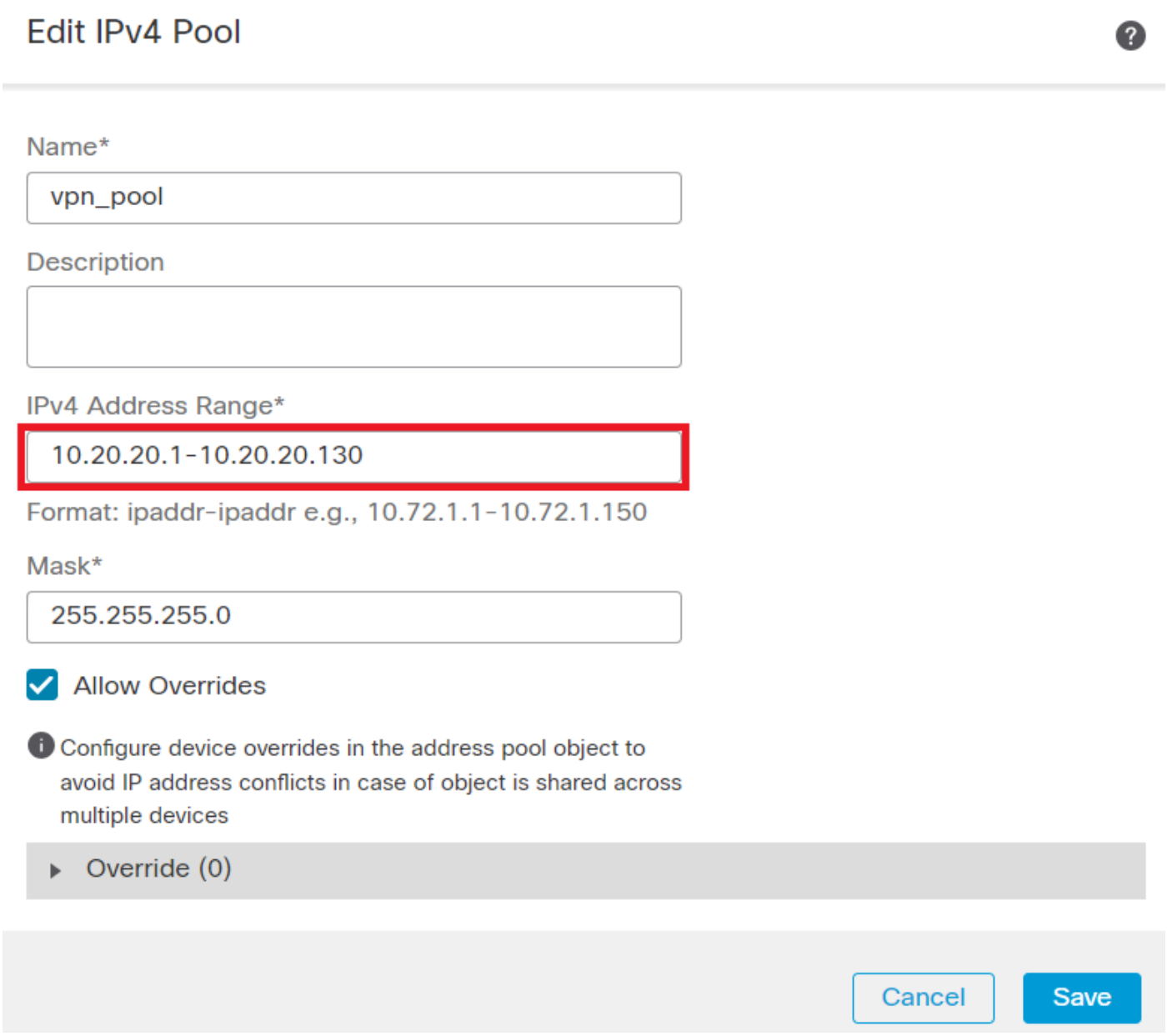


已添加证书

配置VPN用户的地址池

1.导航到对象>对象管理>地址池> IPv4池。

2.输入名称和带掩码的IPv4地址范围。



添加IPv4池

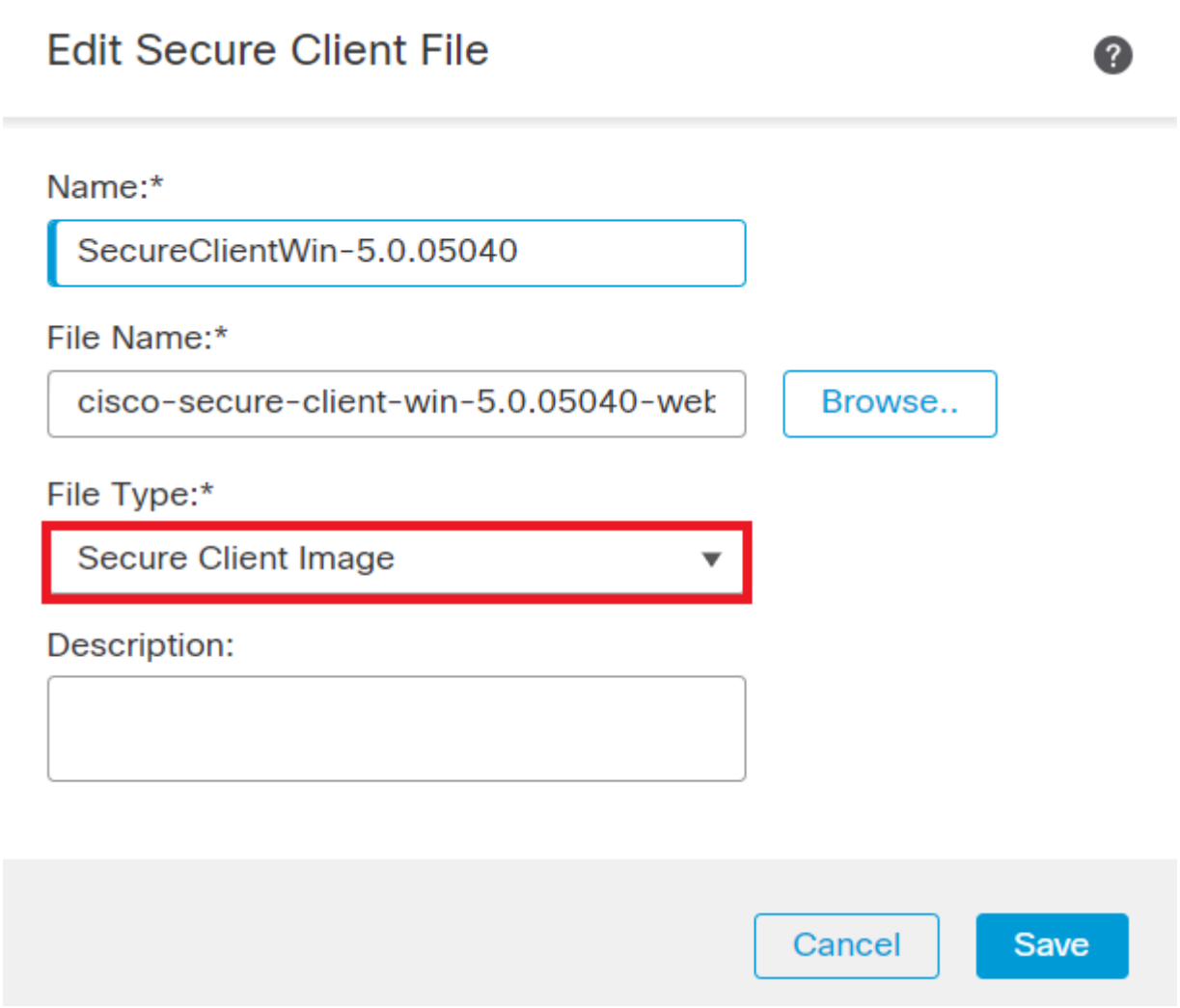
上传安全客户端映像

1.从思科软件站点下载每个操作系统的网络部署安全客户端映像。

2.导航到对象>对象管理> VPN >安全客户端文件>添加安全客户端文件。

3.输入名称，然后从磁盘中选择“安全客户端”文件。

4.将文件类型选择为Secure Client Image，然后单击Save。



添加安全客户端映像

创建和上传XML配置文件

1.从思科软件站点下载并安装安全客户端配置文件编辑器。

2.创建新配置文件，然后从“客户端证书选择”下拉菜单中选择全部。这主要控制存储哪些证书，安全客户端可以根据存储的内容使用哪个证书来读取证书。

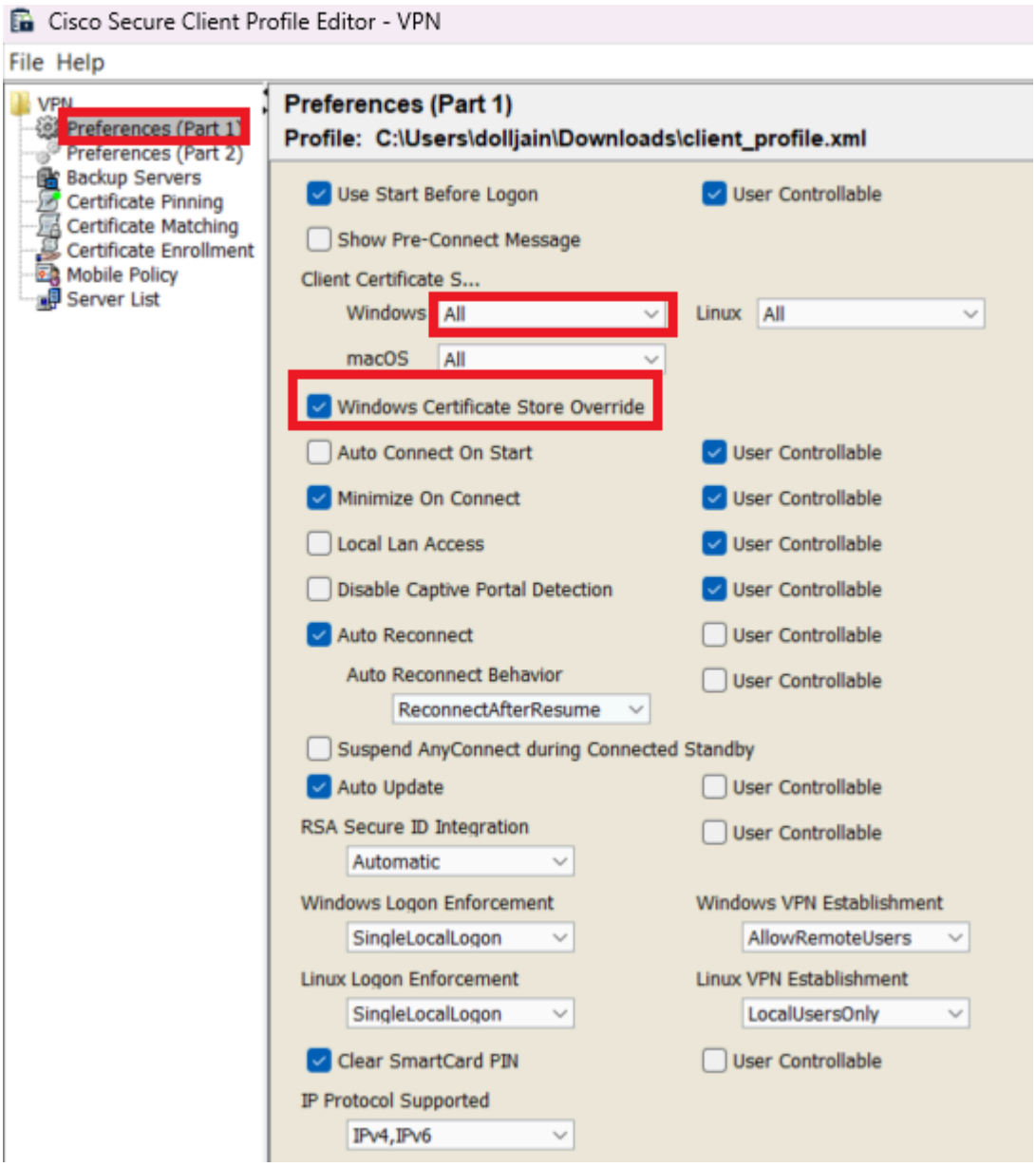
另外两个可用选项是：

i. 计算机:安全客户端仅限于Windows本地计算机证书存储区上的证书查找。

ii. 用户：安全客户端仅限于在本地Windows用户证书存储区中进行证书查找。

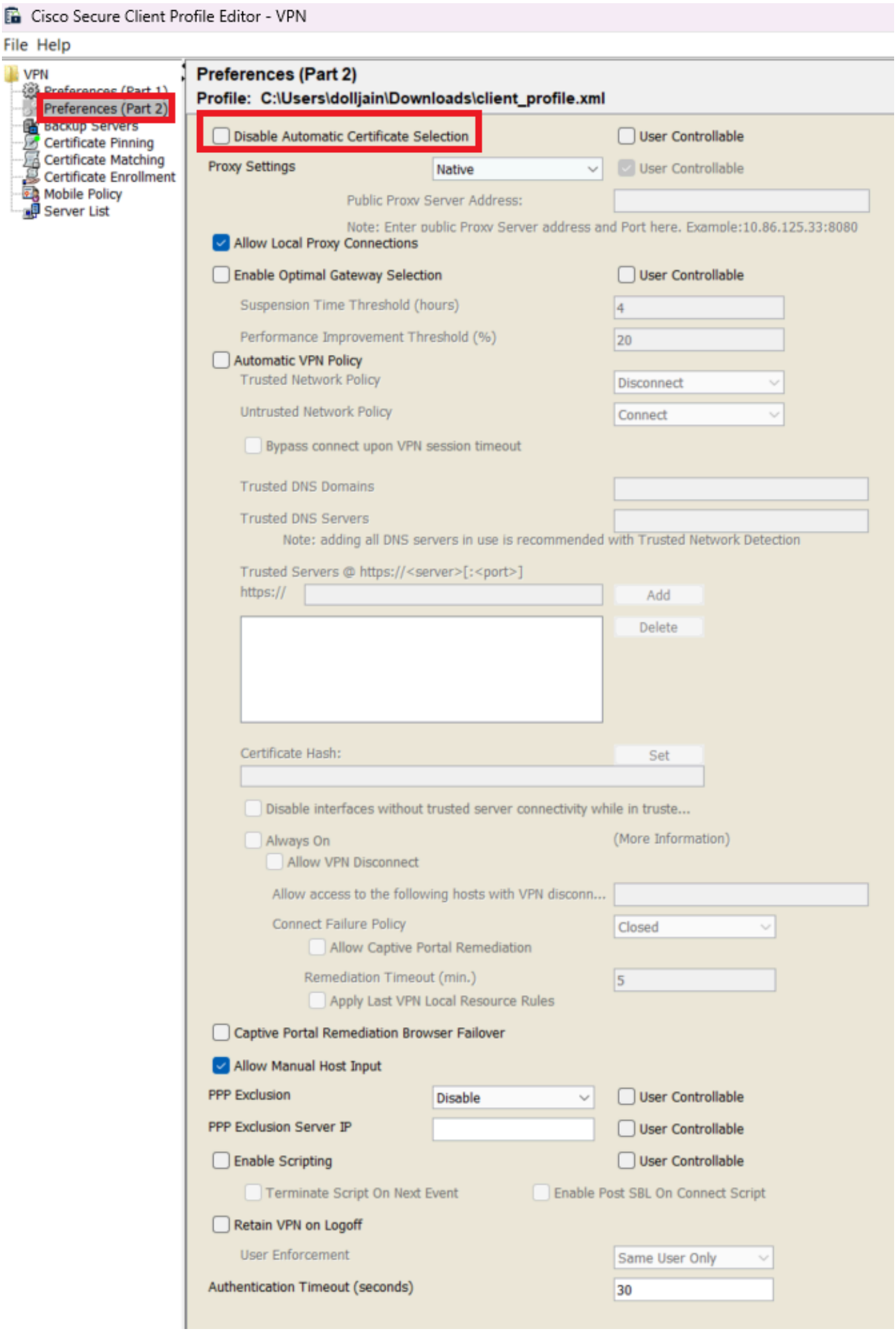
将Certificate Store Override设置为True。

这允许管理员指示安全客户端使用Windows计算机（本地系统）证书存储中的证书进行客户端证书身份验证。默认情况下，证书存储区覆盖仅适用于UI进程中发起连接的SSL。使用IPSec/IKEv2时，安全客户端配置文件中的此功能不适用。



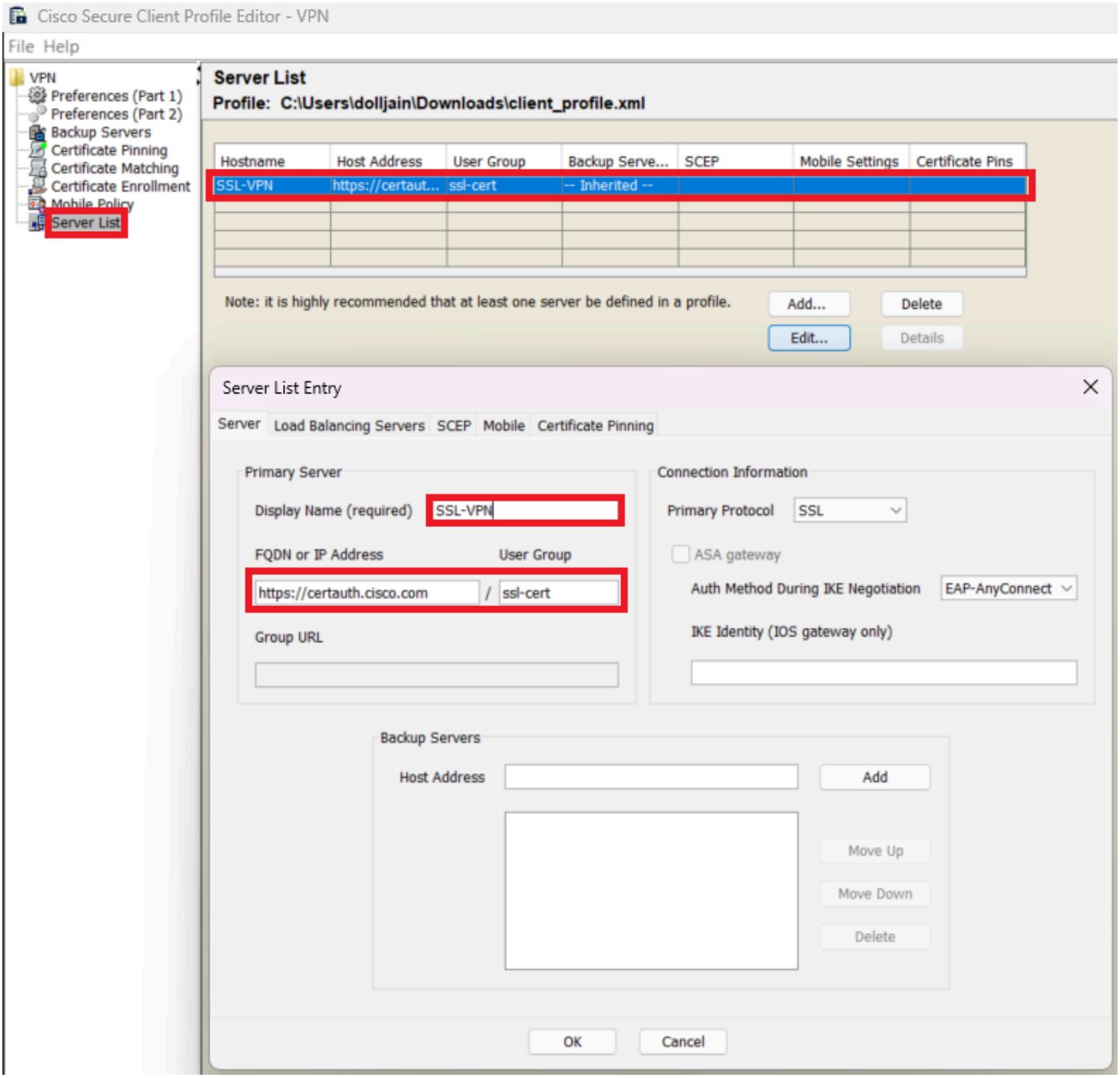
添加首选项（第1部分）

3.（可选）取消选中Disable Automatic Certificate Selection，因为它会避免提示选择身份验证证书。


Cisco Secure Client Profile Editor - VPN
File Help
VPN
Preferences (Part 1)
Preferences (Part 2)
Backup Servers
Certificate Pinning
Certificate Matching
Certificate Enrollment
Mobile Policy
Server List
Preferences (Part 2)
Profile: C:\Users\dolljain\Downloads\client_profile.xml
Disable Automatic Certificate Selection
User Controllable
Proxy Settings
Native
User Controllable
Public Proxy Server Address:
Note: Enter public Proxy Server address and Port here. Example:10.86.125.33:8080
Allow Local Proxy Connections
Enable Optimal Gateway Selection
User Controllable
Suspension Time Threshold (hours)
4
Performance Improvement Threshold (%)
20
Automatic VPN Policy
Trusted Network Policy
Disconnect
Untrusted Network Policy
Connect
Bypass connect upon VPN session timeout
Trusted DNS Domains
Trusted DNS Servers
Note: adding all DNS servers in use is recommended with Trusted Network Detection
Trusted Servers @ https://<server>[:<port>]
https://
Add
Delete
Certificate Hash:
Set
Disable interfaces without trusted server connectivity while in truste...
Always On
(More Information)
Allow VPN Disconnect
Allow access to the following hosts with VPN disconn...
Connect Failure Policy
Closed
Allow Captive Portal Remediation
Remediation Timeout (min.)
5
Apply Last VPN Local Resource Rules
Captive Portal Remediation Browser Failover
Allow Manual Host Input
PPP Exclusion
Disable
User Controllable
PPP Exclusion Server IP
User Controllable
Enable Scripting
User Controllable
Terminate Script On Next Event
Enable Post SBL On Connect Script
Retain VPN on Logoff
User Enforcement
Same User Only
Authentication Timeout (seconds)
30

添加首选项（第2部分）

4.通过在“服务器列表”下提供group-alias和group-url，创建用于在安全客户端VPN中设置配置文件的配置文件并保存XML配置文件Server List Entry。



添加服务器列表

---

5. XML配置文件已可供使用。



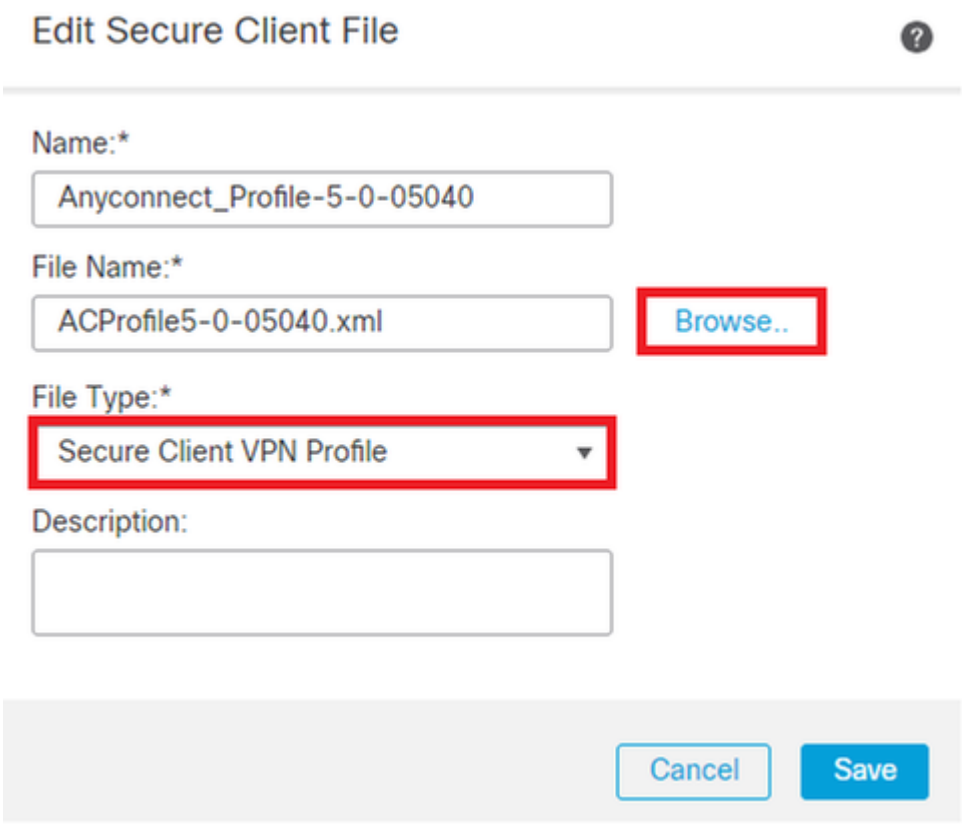
XML配置文件

各种操作系统的XML配置文件的位置：

- Linux - /opt/cisco/anyconnect/profile
- MacOS - /opt/cisco/anyconnect/profile
- Windows - C:\ProgramData\Cisco\Cisco安全客户端\VPN\配置文件

6.导航到对象>对象管理> VPN >安全客户端文件>添加安全客户端配置文件。

7.输入文件的名称，然后单击Browse以选择XML配置文件。单击。Save

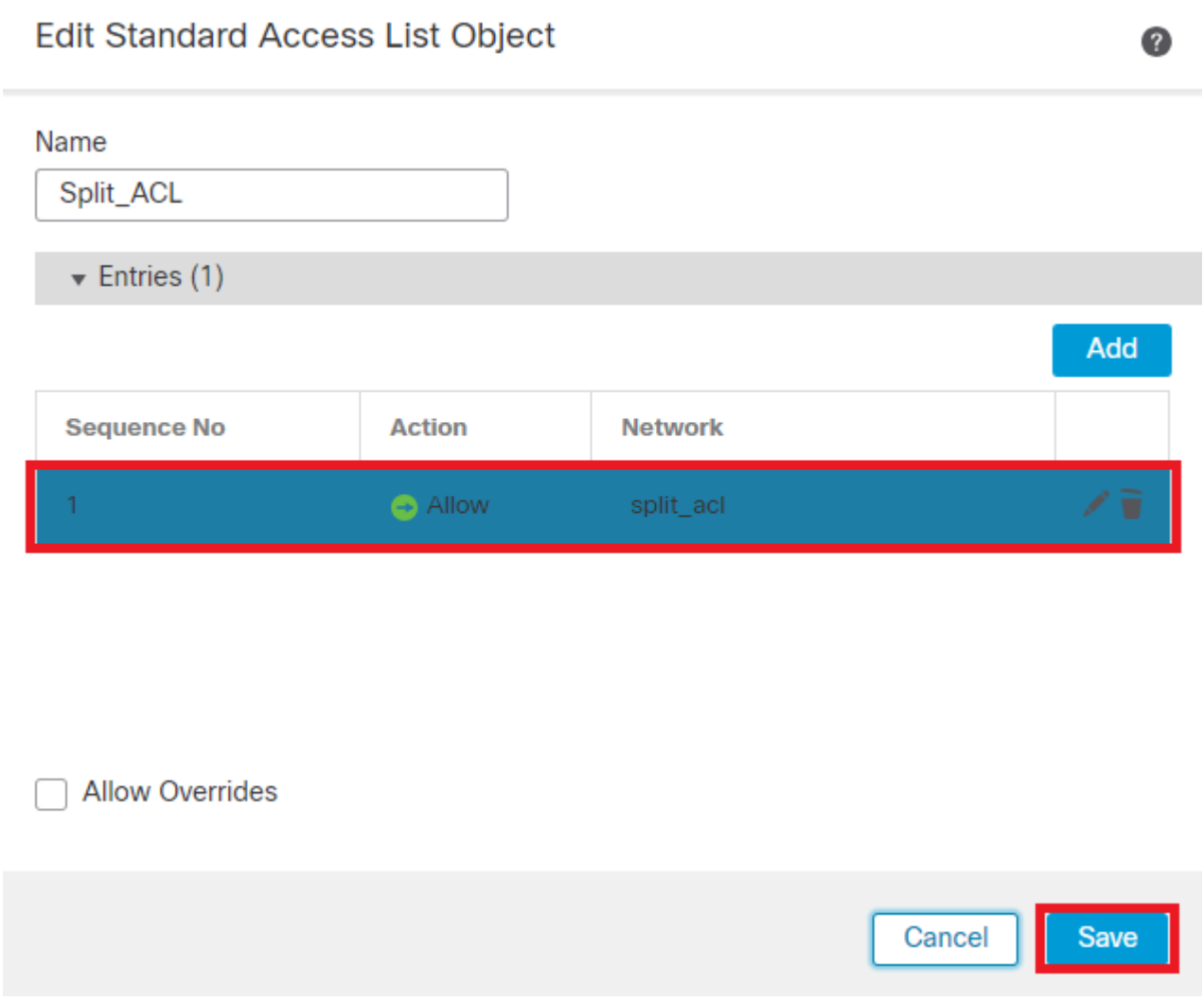


添加安全客户端VPN配置文件

远程访问VPN配置

1.创建ACL以允许访问内部资源。

2.定位至对象>对象管理>访问列表>标准，然后单击添加标准访问列表。

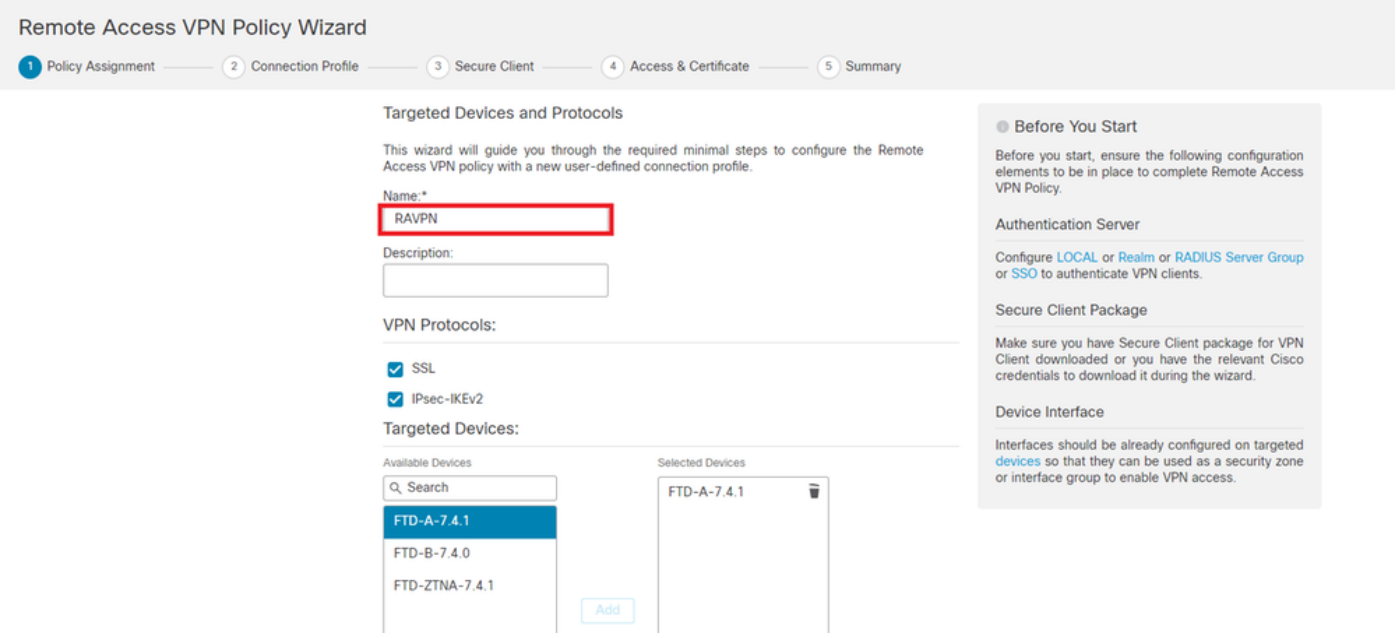


添加标准ACL

注意：安全客户端使用此ACL向内部资源添加安全路由。

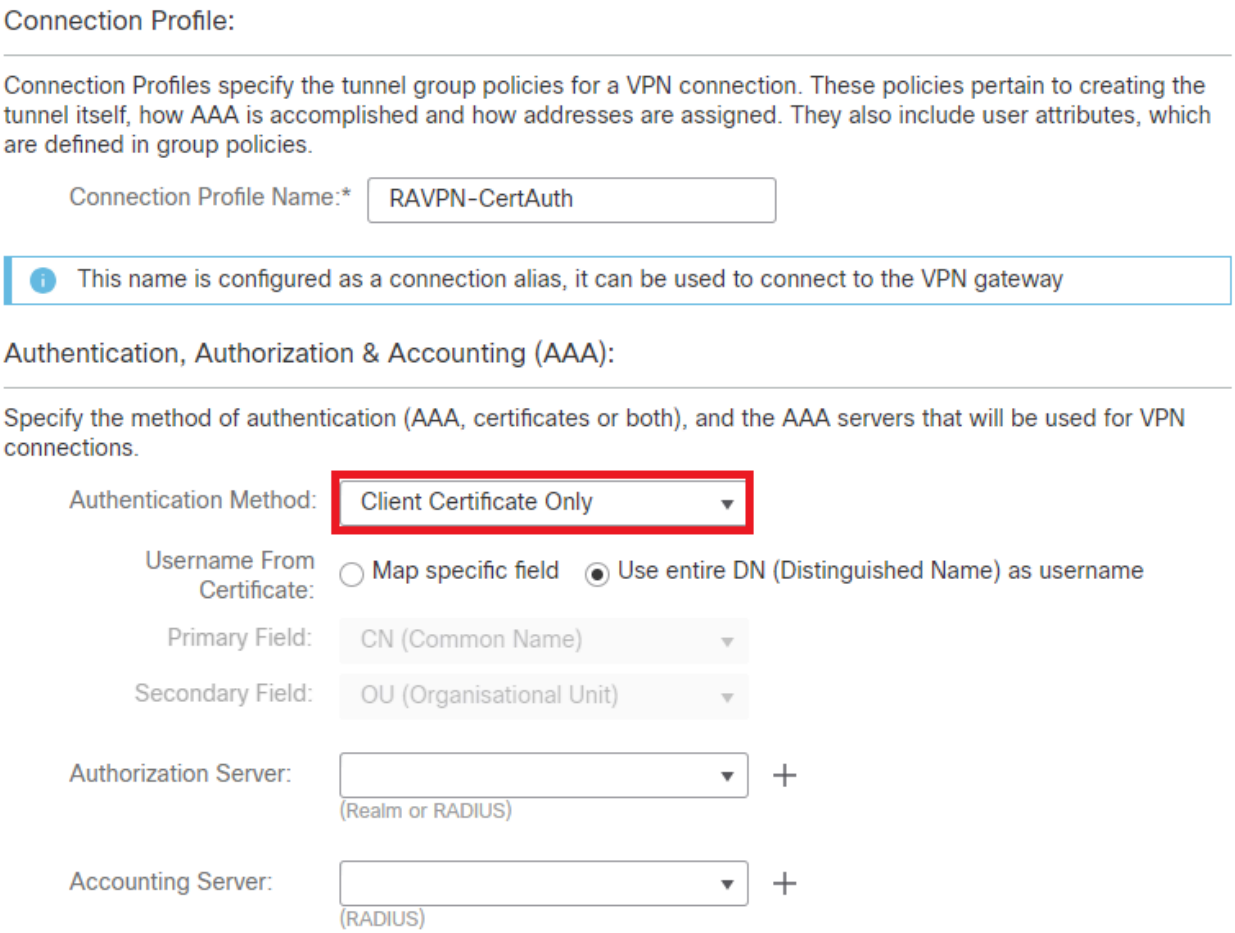
3.导航到设备> VPN >远程访问，然后单击添加。

4.输入配置文件的名称，然后选择FTD设备并单击下一步。



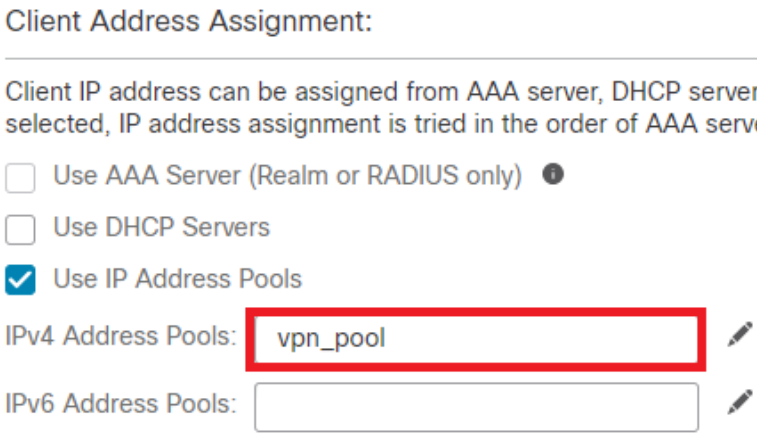
添加配置文件名称

5.输入Connection Profile Name，并在Authentication， Authorization， and Accounting(AAA)下选择Authentication Method as Client Certificate Only。



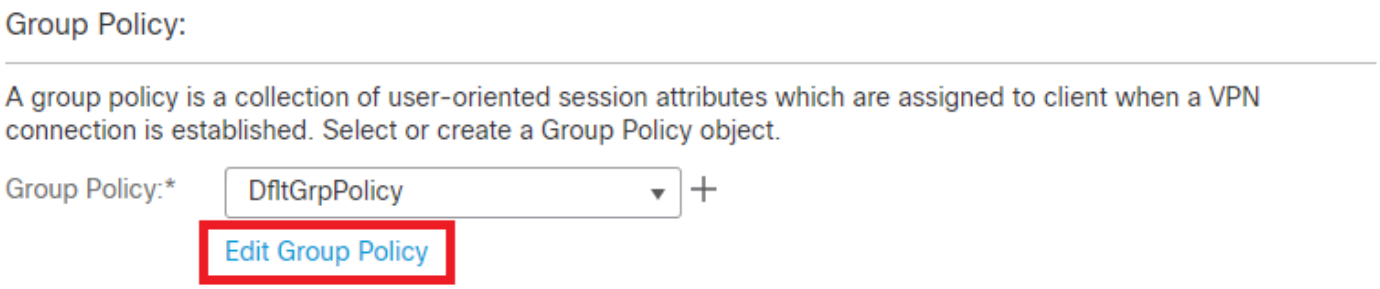
选择身份验证方法

6.单击Client Address Assignment下的Use IP Address Pools，然后选择之前创建的IPv4地址池。



选择客户端地址分配

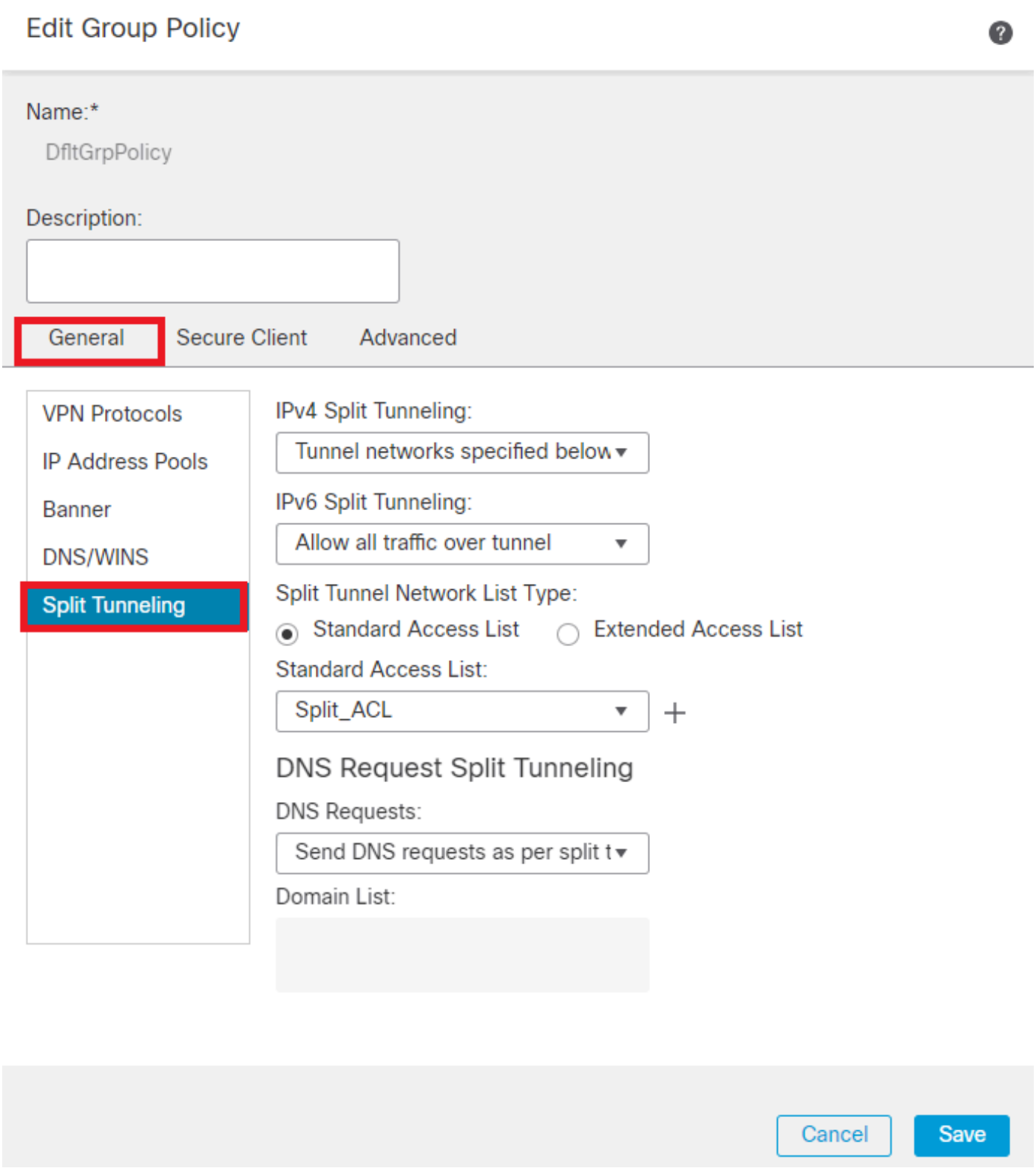
7.编辑组策略。



编辑组策略

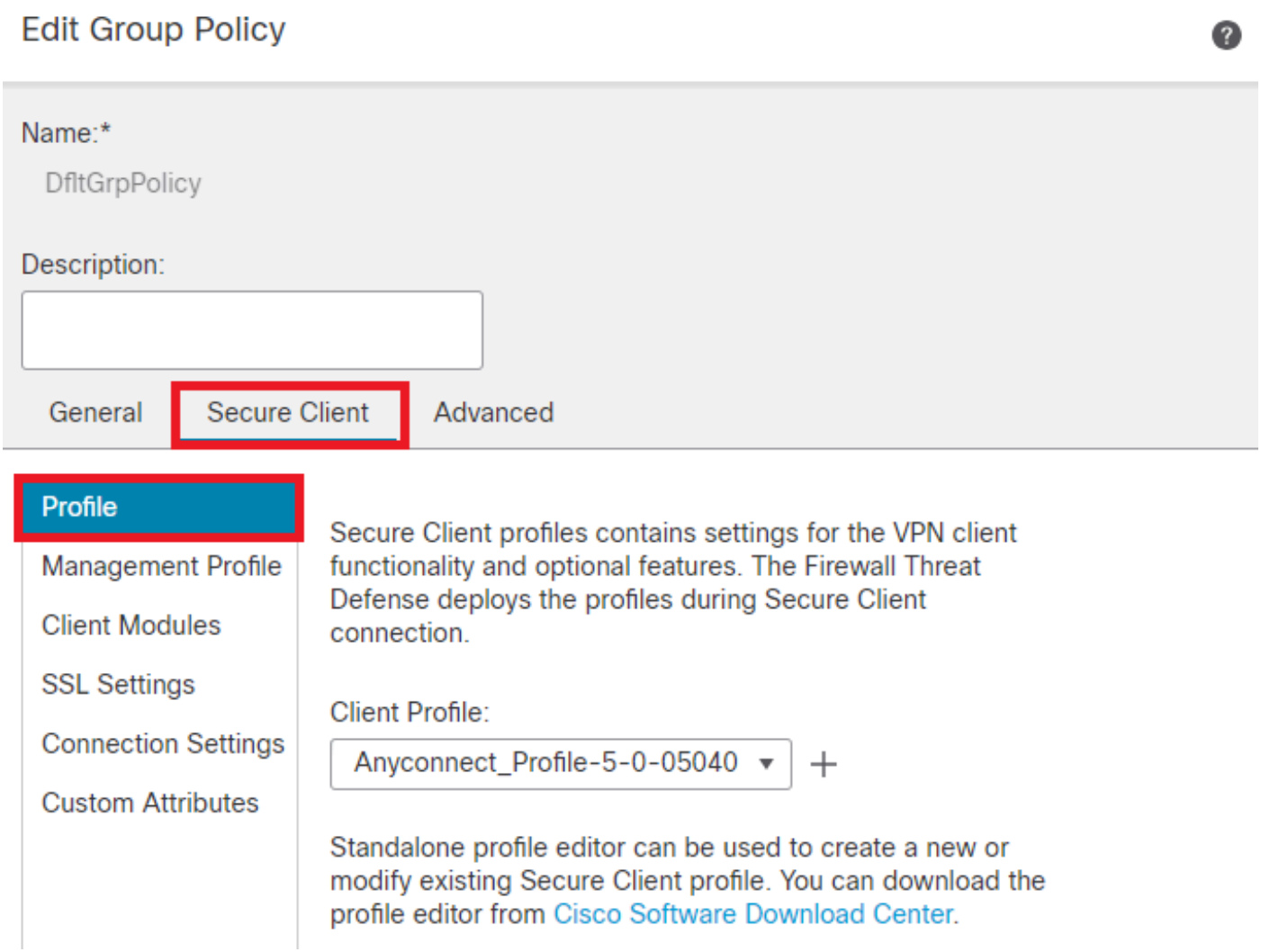
8.导航到General > Split Tunneling，选择下面指定的Tunnel networks，然后在Split Tunnel Network List Type下选择Standard Access List。

9.选择之前创建的ACL。



添加拆分隧道

10.导航到安全客户端>配置文件，选择客户端配置文件，然后单击保存。



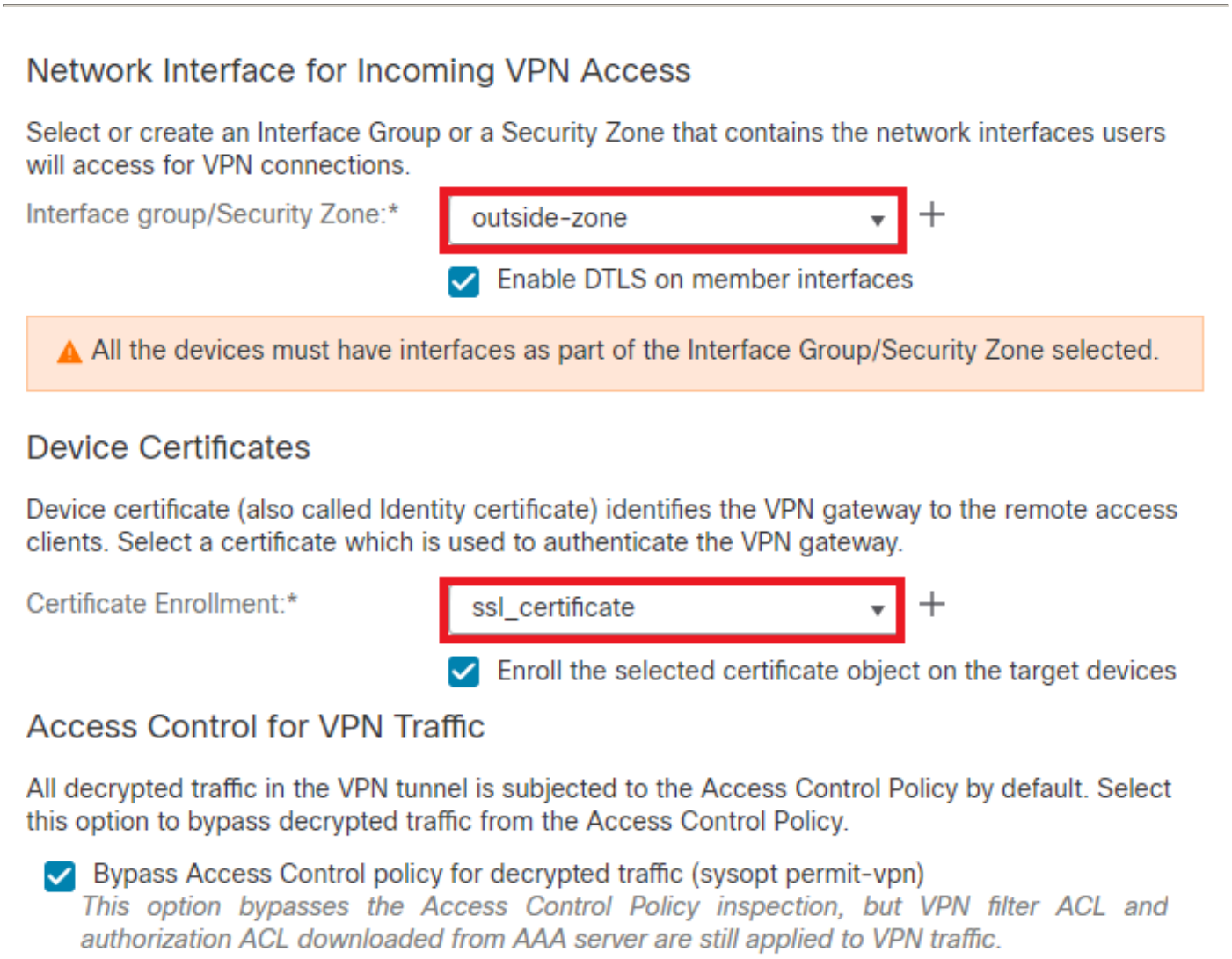
添加安全客户端配置文件

11.单击Next，然后选择Secure Client Image，然后单击Next。



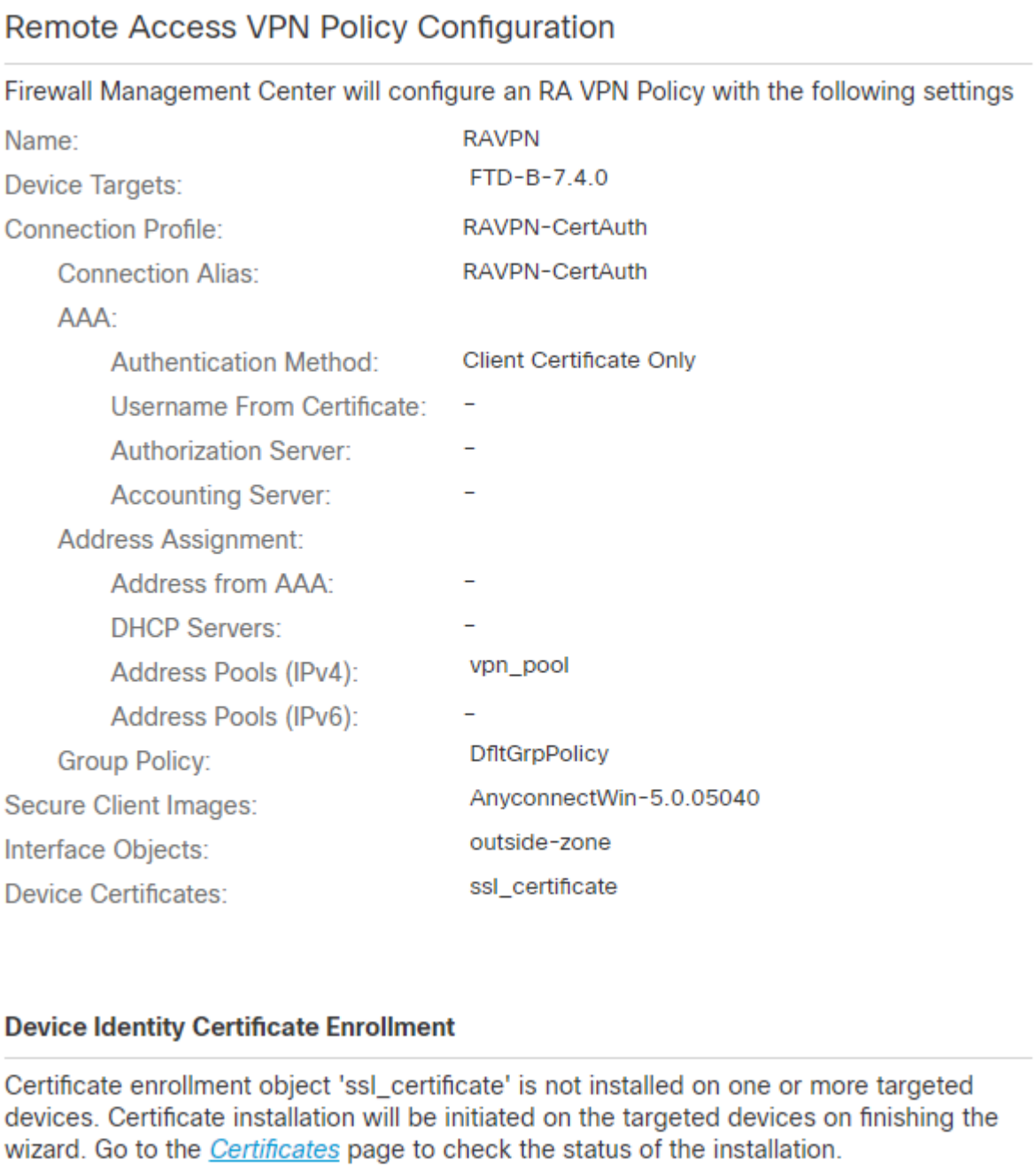
添加安全客户端映像

12.选择Network Interface for VPN Access，选择Device Certificates，选中sysopt permit-vpn，然后单击Next。



为VPN流量添加访问控制

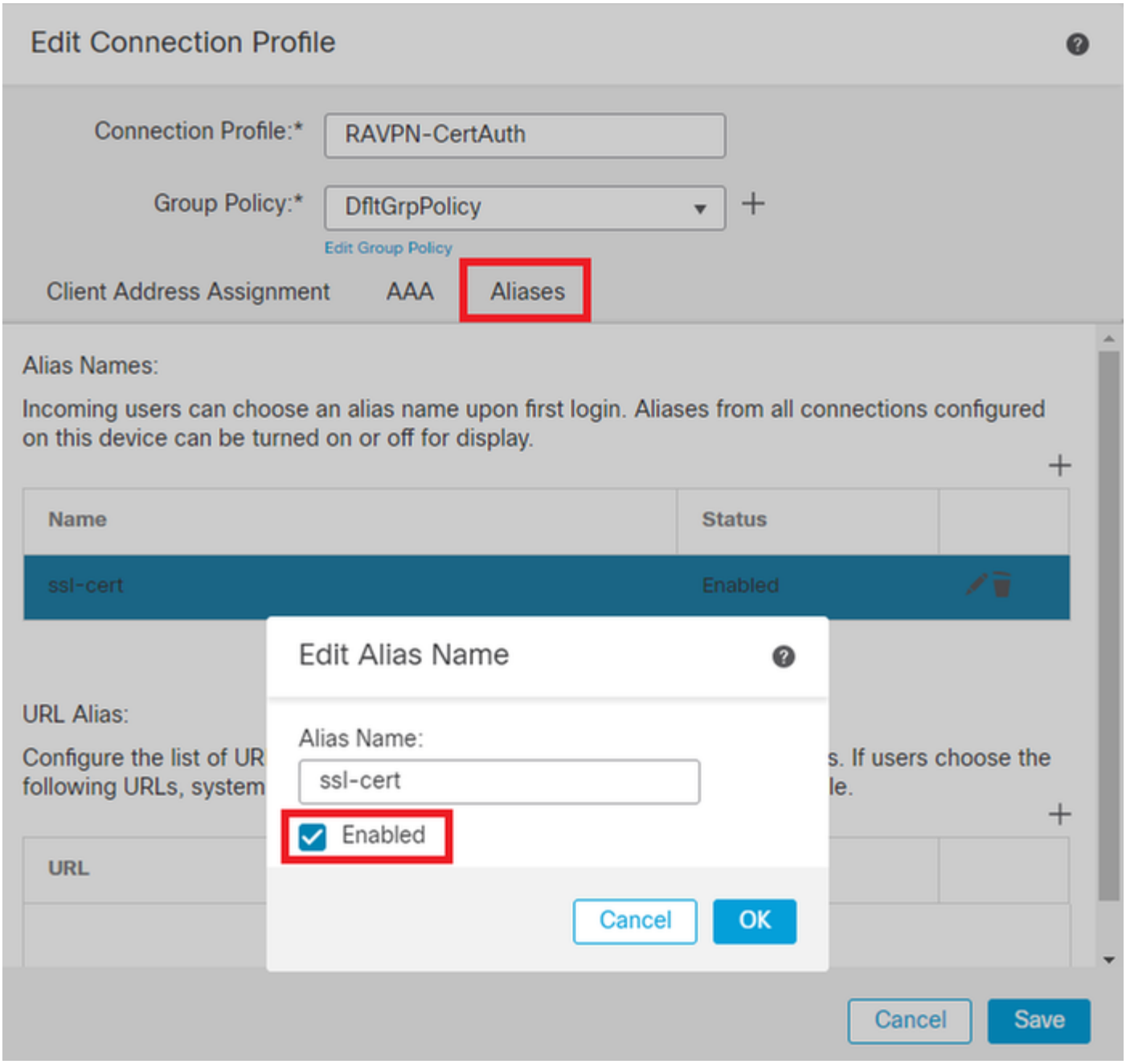
13.检查所有配置，然后单击Finish。



远程访问VPN策略配置

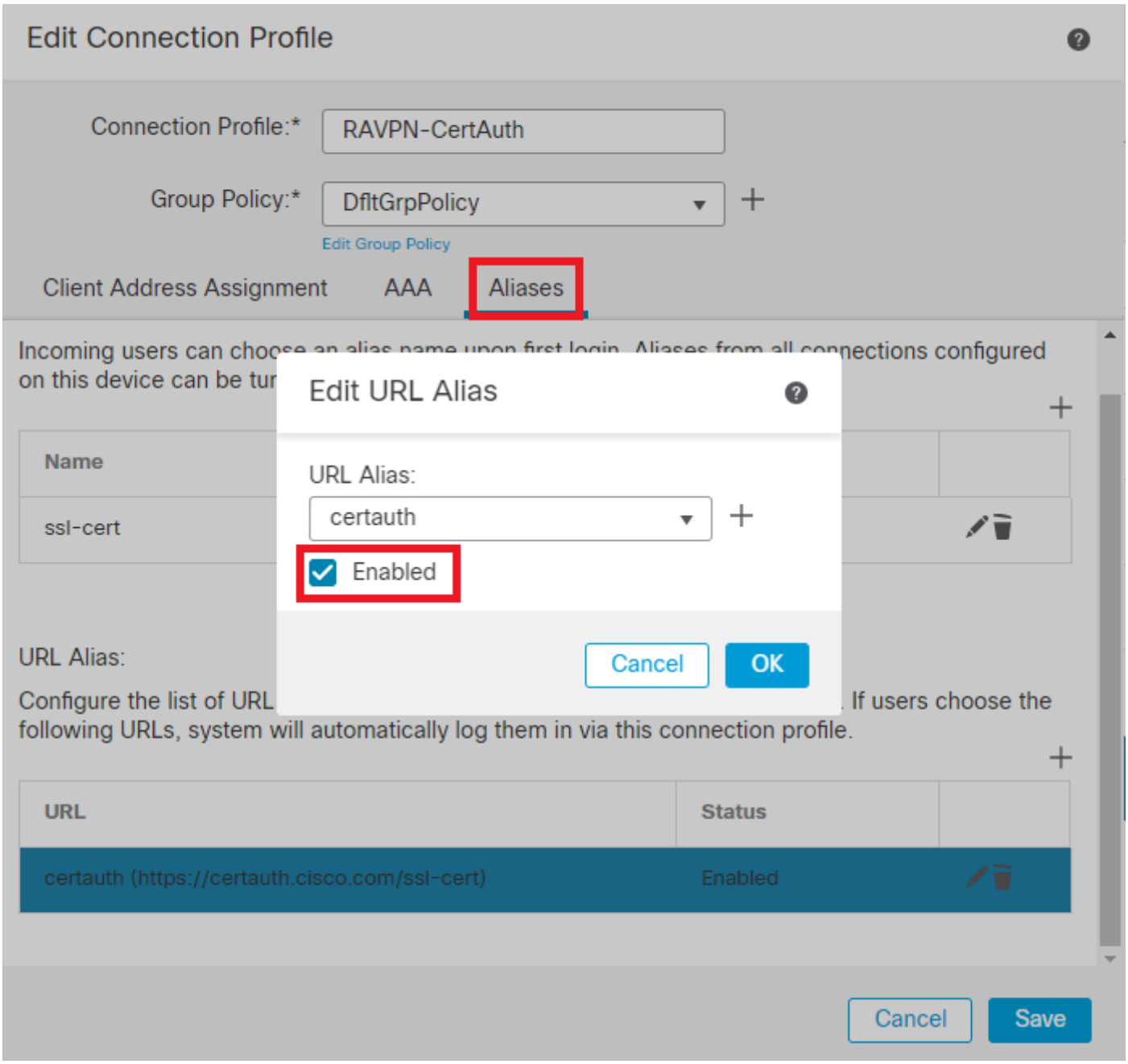
14.完成远程访问VPN的初始设置后，编辑已创建的连接配置文件，然后导航到别名。

15.单击加号图标(+)配置组别名。



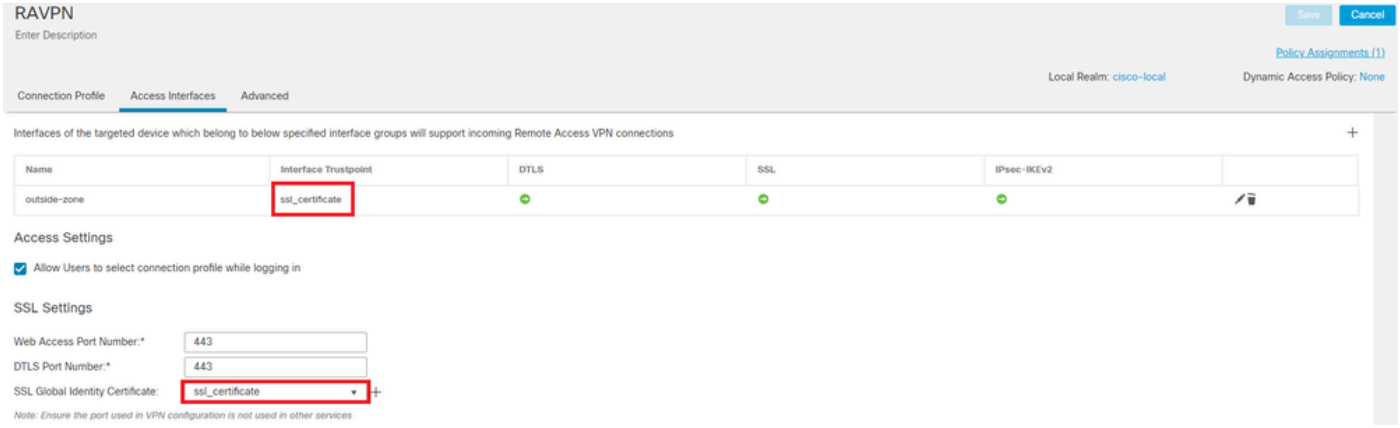
编辑组别名

16.单击加号图标group-url(+)配置。 使用之前在客户端配置文件中配置的相同组URL。



编辑组URL

步骤17.导航到Access Interfaces。在SSL设置下选择Interface Trustpoint和SSL Global Identity Certificate。



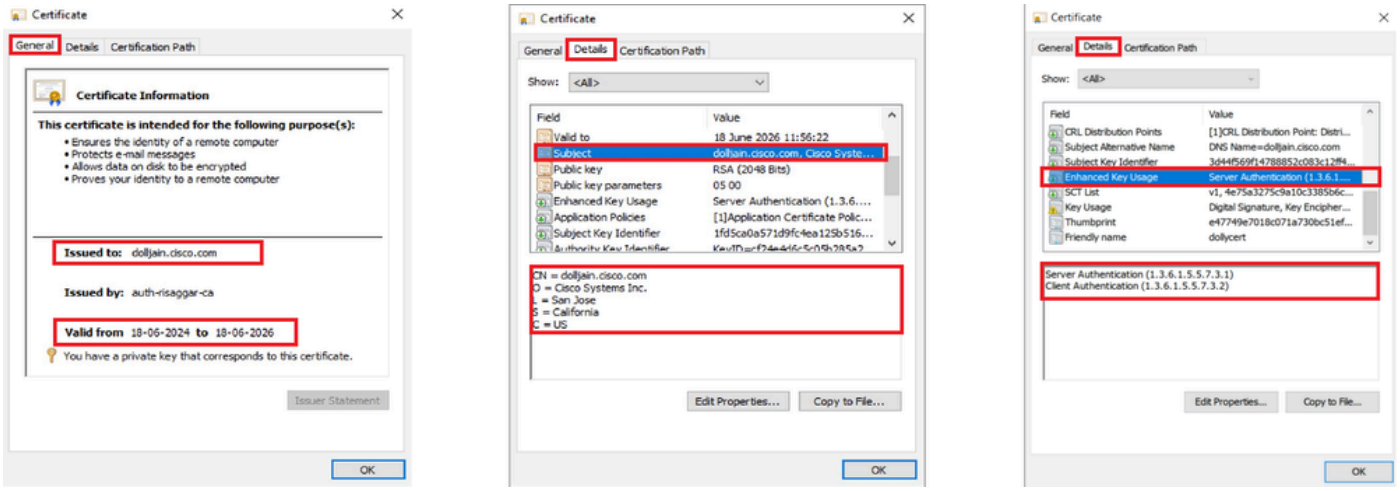
编辑访问接口

18.单击Save并部署更改。

验证

使用本部分可确定配置能否正常运行。

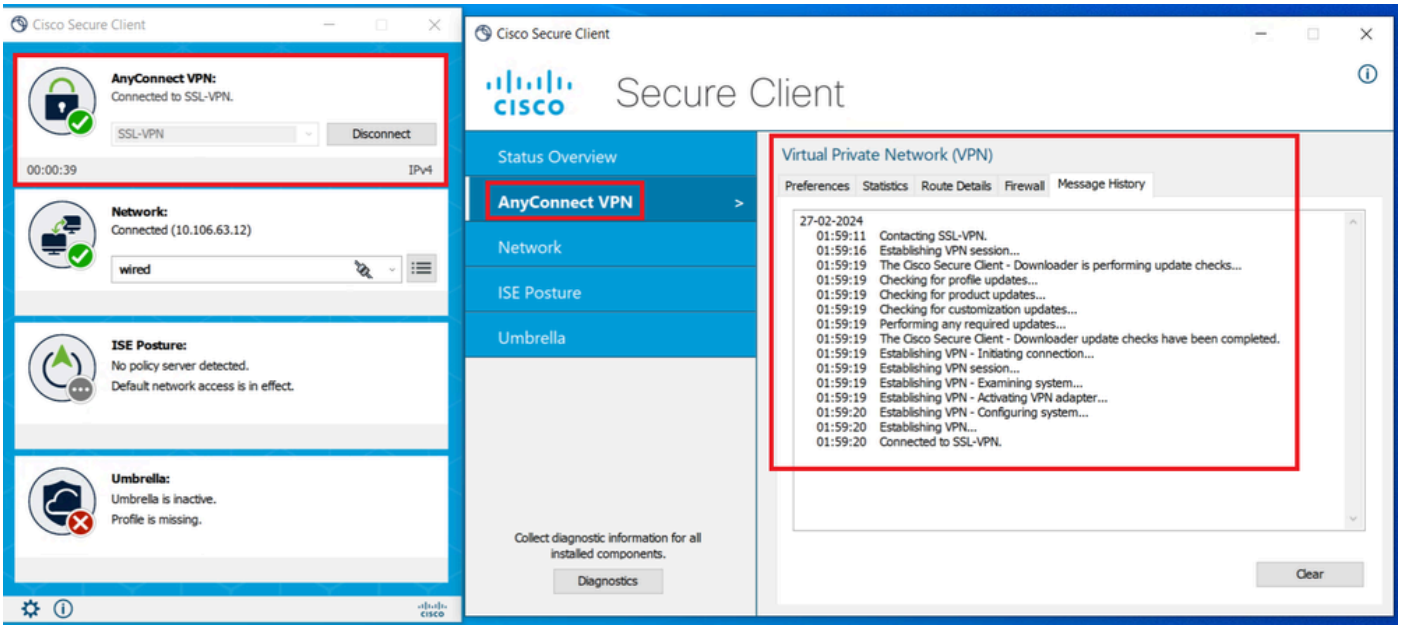
1.安全客户端PC必须在用户PC上安装包含有效日期、主题和增强型密钥使用(EKU)的证书。此证书必须由其证书安装在FTD上的CA颁发，如前所示。在下一个示例中，身份或用户证书由auth-risaggar-ca颁发。



证书亮点

注意：客户端证书必须具有客户端身份验证EKU。

2.安全客户端必须建立连接。



成功的安全客户端连接

3.运行show vpn-sessiondb anyconnect命令，以确认使用过的隧道组下活动用户的连接详细信息。

```
firepower# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : dolljain.cisco.com     Index        : 8
Assigned IP  : 10.20.20.1             Public IP    : 72.163.X.X
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256
Bytes Tx     : 14402                  Bytes Rx     : 9652
Group Policy : DfltGrpPolicy          Tunnel Group : RAVPN-CertAuth
Login Time   : 08:32:22 UTC Mon Mar 18 2024
Duration     : 0h:03m:59s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0ac5de050000800065f7fc16
Security Grp : none                   Tunnel Zone  : 0
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

1.可以从FTD的诊断CLI运行调试：

```
debug crypto ca 14
debug webvpn anyconnect 255
debug crypto ike-common 255
```

2.请参阅Cisco安全客户端VPN常见问题故障排除指南以获取其他帮助。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。